Riigi Infosüsteemi Amet

Intsidendihaldusest ja -haldjatest

25.01.2012

IT Kolledž

Triin Nigul

CERT-EE

Kolm vana tuttavat

- Käideldavus (availability) – andmed on kättesaadavad õigeaegselt ja mugavalt;
- Terviklus (integrity) – andmed on õiged, täielikud ja autentsed;
- Konfidentsiaalsus (confidentiality) – andmed on kättesaadavad ainult selleks volitatud isikutele.

Infoturbeintsident on sündmus, mis võib kahjustada ükskõik millist neist omadustest.

ISKE - turvaklassid

Käideldavus: K0 – töökindlus – pole oluline;

K1 – töökindlus – lubatud summaarne seisak nädalas kuni 1 ööpäev;

K2 – töökindlus – lubatud summaarne seisak nädalas kuni 2 tundi;

K3 – töökindlus – lubatud summaarne seisak nädalas kuni 10 minutit;

Terviklus: T0 – info allikas, muutmise ega hävitamise tuvastatavus ei ole olulised; info õigsuse, täielikkuse ja ajakohasuse kontrollid pole vajalikud;

T1 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; info õigsuse, täielikkuse, ajakohasuse kontrollid erijuhtudel ja vastavalt vajadusele;

T2 – info allikas, selle muutmise ja hävitamise fakt peavad olema tuvastatavad; vajalikud on perioodilised info õigsuse, täielikkuse ja ajakohasuse kontrollid;

T3 – infol allikal, selle muutmise ja hävitamise faktil peab olema tõestusväärtus; vajalik on info õigsuse, täielikkuse ja ajakohasuse kontroll reaalajas.

Konfidentsiaalsus: S0 – avalik info: juurdepääsu teabele ei piirata (st lugemisõigus kõigil huvitatutel, muutmise õigus määratletud tervikluse nõuetega);

S1 – info asutusesiseseks kasutamiseks: juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral;

S2 – salajane info: info kasutamine lubatud ainult teatud kindlatele kasutajate gruppidele, juurdepääs teabele on lubatav juurdepääsu taotleva isiku õigustatud huvi korral,

S3 – ülisalajane info: info kasutamine lubatud ainult teatud kindlatele kasutajatele,

Infoturbeintsident

ISO 27001: Soovimatu või ootamatu infoturbesündmus (või infoturbesündmuste sari), mis arvestatava tõenäosusega rikub põhitegevuse operatsioone ja ähvardab teabe turvalisust.

ITIL: Iga IT teenuse mitteplaanitud katkestus või IT teenuse kvaliteedi halvenemine. Konfiguratsioonielemendi tõrge, kus IT teenus veel mõjutatud pole, on samuti intsident.

NIST: IT turva- ja kasutuspoliitikate või standardsete turvapraktikate rikkumine või vahetu oht selleks.

ISKE: Sündmus ja/või sündmused, millega kaasneb andmete ja/või muude infovarade käideldavuse, tervikluse ja/või konfidentsiaalsuse kadu ja/või tekib oluline oht andmete käideldavuse, tervikluse ja/või konfidentsiaalsuse kao tekkeks; /.../ turvaintsidendiks nimetatakse sündmust, mille tagajärjel võib tekkida suur kahju.

HOS (hädaolukord): Sündmus või sündmuste ahel, mis ohustab paljude inimeste elu või tervist või põhjustab suure varalise kahju või suure keskkonnakahju või tõsiseid ja ulatuslikke häireid elutähtsa teenuse toimepidevuses ning mille lahendamiseks on mille lahendamiseks on vajalik mitme asutuse või nende kaasatud isikute kiire kooskõlastatud tegevus.

Intsidentide tüübid (ISKE)

Turvaintsidentidega kaasnevad võimalikud kahjud võivad mõjutada nii andmete konfidentsiaalsust või terviklust kui ka nende käideldavust.

Turvaintsidendid võivad esineda alljärgnevatel juhtudel:

- kasutaja vale käitumine, mille tagajärjeks on andmete kadu või turvakriitiline süsteemiparameetrite muutumine,
- turvaaukude esinemine riist- või tarkvarakomponentides,
- massiline viiruste esinemine, Loveletteri näide
- internetiserverite ründamine, 2007 näide on kõiki ära tüüdanud
- konfidentsiaalsete andmete avalikustamine, KOLA näide
- personali puudumine või
- kriminaalne tegevus (nagu sissemurdmine, vargus või väljapressimine seoses IT-ga).

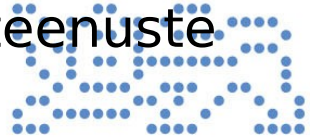
Millal sündmusest saab intsident - teenustaseme kokkulepe (SLA)

ITIL: Intsidendiks nimetatakse iga IT teenuse mitteplaneeritud katkestust või IT teenuse kvaliteedi halvenemist. Konfiguratsioonielemendi tõrge, kus IT teenus veel mõjutatud ei ole, on samuti intsident.

Intsidentide haldus on protsess, mis käsitleb kõiki intsidente nagu süsteemide ja teenuste tõrked, klientide märkused ja päringud, tehnilise personali tähelepanekud ja automaatsed seiresüsteemi teated.

Eesmärk on taastada normaalne teenus (SLA-s määratud näitajatega) nii kiiresti kui võimalik ja minimiseerides sealjuures ebasoovitavaid mõjusid äriprotsessidele.

Intsidendihaldus **käsitleb** kõiki **sündmusi**, mis ei ole normaalse haldusprotsessi osa ja mis on esile kutsunud või mis võivad esile kutsuda ebasoovitavaid hälbeid IT teenuste kvaliteedile.



Mitte kõik sündmused ja kasutajapöördumised ei ole intsidendid.

Kokkuvõtlikult

- Ettevalmistus

Turvapoliitikad ja -protseduurid, turvauuendused, masinate ja võrguturve, pahavara tõkestamine, kasutajate teadlikkuse tõstmine

Intsidendi lahendamise vahendite soetamine ja koolitus

- Intsidendi avastamine, kinnitamine

Intsidendi kategooriad, intsidendi „tunnused“, intsidendi kriitilisus

- Lokaliseerimine, ohjeldamine
- Analüüs, lahendamine, taaste
- Kommunikatsioon (läbib iga etappi)
- Järeltegevused: hindamine, raporteerimine, meetmete täiendamine

Kasulikke näpunäiteid

- Lase kasutajal pool dokumenteerimistööst ära teha – võta kasutusele kasutajapöördumiste haldamise süsteem
- Kui intsidendi kohta on tulnud juba mitu sõnumit, saada süsteemi kasutajatele e-kiri probleemi kohta – nii väldid katkematut hädakisa
- Ära unusta kriitilisest intsidendist teavitada asutuse võtmeisikuid – loo nn SMS-grupp meilisüsteemi
- Sõnumisse lisa ka esialgne prognoos, milliseks hetkeks intsident lahendatud saab (pigem väikse varuga) – saad rahulikult tööd teha
- Andmete turvaklassid, teenustaseme kokkulepped jms on tegelikult sulle abiks – nii turvameetmete plaanimisel kui intsidendi kriitilisuse määramisel
- Intsidendi aruandesse lisa soovitused e ettepanekud intsidendi kordumise vältimiseks – kui sinu nõu kuulda ei võetud, vastutab analoogse intsidendi kordumisel juba keegi teine
- Iial ei tea, mis elu toob, juba homme võib sinu tööandjaks olla keegi teine – ära tee oma järeltulija elu ülikeeruliseks – ole

Miks dokumenteerida - ISKE

Turvaprobleemi kõrvaldamise ajal tuleks kõik läbiviidud toimingud võimalikult üksikasjalikult ning ideaalsel juhul standardiseeritult dokumenteerida:

et saada ülevaade põhjustest, tagajärgedest ja meetmetest,

et selgitada esinevaid probleeme,

et oleks võimalik kõrvaldada viga, mis võib ette tulla kiire vastumeetmete rakendamise korral,

et oleks võimalik juba tuntud probleeme nende korduval esinemisel kiiremini kõrvaldada,

et oleks võimalik turvaauke likvideerida ja ennetavaid meetmeid välja töötada ning

et koguda võimaliku kriminaaljälituse jaoks tõendeid.

Sellise dokumentatsiooni hulka ei kuulu mitte ainult läbiviidud toimingute kirjeldus koos ajakava ja osalevate isikute nimedega, vaid ka intsidendist puudutatud IT-süsteemide logifailid.

Turvaintsidentide dokumentide konfidentsiaalsust tuleb sobival viisil kaitsta.

Turvaintsidendi raporti näidisvorm

Täname!